Commonwealth of Massachusetts
Center for Health Information & Analysis (CHIA)
Government Agency Application for Data

This application is to be used by agencies, departments or authorities of the Commonwealth of Massachusetts, as well as federal agencies and departments of the United States of America ("Government Agencies"). Data requests from other states, as well as other political subdivisions of the Commonwealth of Massachusetts must use the Non-Government Agency Application form.

I. GENERAL INFORMATION

APPLICANT INFORMATION	
Applicant Name:	
Title:	
Organization:	
Project Title:	
Date of Application:	
Objectives (240 character limit)	

II. PROJECT SUMMARY

Briefly identify the public purpose(s) for which CHIA data are sought and how you will use the requested data to accomplish your purpose(s). Please include (or attach) a brief description of your methodology. If your project will require linking CHIA data to another dataset, please identify all linkages proposed and explain the reason(s) that the linkage is necessary to accomplish the purpose of the project. If applicable, please identify the specific steps you will take to prevent the identification of individual patients in the linked dataset.

III. FILES REQUESTED

Please indicate the databases from which you seek data, the Level(s) and Year(s) of data sought.

ALL PAYER CLAIMS DATABASE	Level 1[1] or 2[2]	Single or Multiple Use	Year(s) Of Data Requested Current Yrs. Available 2009 - 2012
☐ Medical Claims	☐ Level 1 ☐ Level 2	Multiple	☐ 2009 ☐ 2010 ☐ 2011 ☐ 2012
☐ Pharmacy Claims	☐ Level 1 ☐ Level 2		☐ 2009 ☐ 2010 ☐ 2011 ☐ 2012

[1] Level 1 Data: De-identified data containing information that does not identify an individual patient and with respect to which there is no reasonable basis to believe the data can be used to identify an individual patient. This data is de-identified using standards and methods required by HIPAA.

[2] Level 2 (and above) Data: Includes those data elements that pose a risk of re-identification of an individual patient.

☐ Dental Claims ☐ Member Eligibility ☐ Provider ☐ Product	☐ Level 2 ☐ Level 2 ☐ Level 2 ☐ Level 2	Select... Select... Select... Select...	☐ 2009 ☐ 2010 ☐ 2011 ☐ 2012

CASEMIX	Level 1 - 6	Fiscal Years Requested
Inpatient Discharge	☐ Level 1 – No Identifiable Data Elements ☐ Level 2 – Unique Physician Number (UPN) ☐ Level 3 – Unique Health Information Number (UHIN) ☐ Level 4 – UHIN and UPN ☐ Level 5 – Date(s) of Admission; Discharge; Significant Procedures ☐ Level 6 – Date of Birth; Medical Record Number; Billing Number	1998-2012 Available (limited data 1989-1997)
Outpatient Observation	☐ Level 1 – No Identifiable Data Elements ☐ Level 2 – Unique Physician Number (UPN) ☐ Level 3 – Unique Health Information Number (UHIN) ☐ Level 4 – UHIN and UPN ☐ Level 5 – Date(s) of Admission; Discharge; Significant Procedures ☐ Level 6 – Date of Birth; Medical Record Number; Billing Number	2002-2012 Available
Emergency Department	☐ Level 1 – No Identifiable Data Elements ☐ Level 2 – Unique Physician Number (UPN) ☐ Level 3 – Unique Health Information Number (UHIN) ☐ Level 4 – UHIN and UPN; Stated Reason for Visit ☐ Level 5 – Date(s) of Admission; Discharge; Significant Procedures ☐ Level 6 – Date of Birth; Medical Record Number; Billing Number	2000-2012 Available

IV. REQUESTED DATA ELEMENTS [APCD]

State and federal privacy laws limit the use of individually identifiable data to the minimum amount of data needed to accomplish a specific project objective. Please use the APCD Data Specification Workbook to identify which data elements you would like to request and attach this document to your application.

V. MEDICAID DATA [APCD Only]

Please indicate here whether you are seeking Medicaid Data:

○ Yes

○ No

Federal law (42 USC 1396a(a)7) restricts the use of individually identifiable data of Medicaid recipients to uses that are directly connected to the administration of the Medicaid program. If you are requesting Medicaid data from Level 2 or above, please describe in detail why your use of the data meets this requirement. Applications requesting Medicaid data will be forwarded to MassHealth for a determination as to whether the proposed use of the data is directly connected to the administration of the Medicaid program. MassHealth may impose additional requirements on applicants for Medicaid data as necessary to ensure compliance with federal laws and regulations regarding Medicaid.

Government agencies approved to receive Medicaid data will be required to execute an Addendum to CHIA's standard data use agreement, containing terms and conditions required by CHIA's data sharing agreement with MassHealth.

VI. MEDICARE DATA

Please indicate here whether you are seeking Medicare Data:

○ Yes

○ No

Medicare data may only be disseminated to state agencies and/or entities conducting research projects that are directed and partially funded by the state if such research projects would allow for a Privacy Board or an IRB to make the findings listed at 45 CFR 164.512(i)(2)(ii) if the anticipated data recipient were to apply for the data from CMS directly. If you are requesting Medicare data, please describe in detail why your proposed project meets the criteria set forth in 45 CFR 164.512(i)(2)(ii). Applicants must describe how they will use the data and inform CHIA where the data will be housed. CHIA must be informed if the data has been physically moved, transmitted, or disclosed.

Applicants seeking Medicare data must complete a Medicare Request Form.

Applicants approved to receive Medicare data will be required to execute an Addendum to CHIA's standard data use agreement, containing terms and conditions required by CHIA's data use agreement with CMS.

VII. DIRECT PATIENT IDENTIFIERS[3]

State and federal privacy laws may require the consent of Data Subjects prior to the release of any Direct Patient Identifiers. If you are requesting data that includes Direct Patient Identifiers, please provide documentation of patient consent or your basis for asserting that patient consent is not required.

VIII. DATA SECURITY AND INTEGRITY

(Information provided in this section is confidential and not a public record.)

Complete this section for each location where the data will be stored or accessed. If you plan to use an agent/contractor that has access to the data at a location other than your location or in an off-site server and/or database, the agent/contractor should complete this section.

[3] Direct Patient Identifiers. Personal information, such as name, social security number, and date of birth, that uniquely identifies an individual or that can be combined with other readily available information to uniquely identify an individual.

1. *Physical Location of the data*: Please provide the delivery address for the data, as well as the full address, including building and floor, of each location where data will be stored.

2. *Person Responsible for securing the data:* Please provide the name and contact information of the individual responsible for securing the data.

3. *Information Security Compliance:*
   a. Commonwealth of Massachusetts government agencies: Is your agency compliant with Massachusetts Executive Order 504?
   - ☐ Yes
   - ☐ No

   b. U.S. government agencies: Is your agency compliant with FISMA?
   - ☐ Yes
   - ☐ No

4. *Encryption of copied data:* Will the APCD data or any copy of the data be copied from the encrypted hard drive to another storage medium? If yes, is the storage medium encrypted? With what level of encryption (e.g., AES 256 bit)?

5. *Software Applications Accessing the Data:* What is the provider (company, etc.), product name, and version of the software application used to access and manipulate the data? If this software application is a *custom* application (i.e., developed in-house or by a third party specifically for your organization) then attach all development documentation relevant to its authorization, authentication, and other security features and capabilities (functional specification(s), security design review, security architecture and workflow diagrams, security test plan(s), security code review(s), etc.).

6. *Technical Safeguards*: What additional specific technical safeguards (not mentioned in prior answers) will be used to *mitigate* the risk of unauthorized access to each of the following:

   a) The original data media and subsequent copies of the data, including backups of the data.

b) Any work, scratch, or temporary files generated from the data.

c) Any device (appliances, workstations, servers, et al) with Internet connectivity which can also connect internally to any other device containing the data or a copy of the data.

7. *Portable Computing Devices*: How will you prevent *all* portable computing devices (laptops, tablets, notebooks, netbooks, smartphones et al), whether owned or issued by your organization or other parties or persons, from gaining access to, or storing, the data or copies of the data?

8. *Administrative Safeguards*: If your agency has a Written Information Security Program (WISP) or an information security policy(ies) that contains data security provisions, please attach the document(s) and refer to the applicable sections in your response to the questions below.

9. List any additional technical information security or privacy safeguards your organization has pertinent to mitigating the risk of unauthorized access to or use of the data.

10. *Enterprise Information Security (*to be completed by the agency's Information Security Officer or equivalent):

    a. Name: _____

    b. Title: _____

    c. On the system that will access the data, is an audit log maintained of all user logons to the system [Y/N]? How many days of activity are preserved in the log? _____

    d. Are all the user accounts that log on to any machine (server or endpoint) that accesses the data uniquely assigned to individual users (i.e., the user accounts are not shared)? [Y/N]

    e. Do you run an anti-virus or anti-malware product on the server that will host the data [Y/N]? If Yes, is the software at a current patch/revision/version level? If no, what is the product name and patch/revision/version number? _____

    f. Check all the security features of the room containing the server hosting the APCD data or a copy of it:

        i. ☐ Continuous live recorded video with server in field of view

ii. ☐ Access log of all individuals entering the room

iii. ☐ Secure server rack

iv. ☐ Locked room

IX. ASSURANCES

Government Agencies requesting and receiving data from CHIA will be provided with data following the execution of a data use agreement, or pursuant to a specific data sharing agreement referenced herein, that requires the agency to adhere to processes and procedures aimed at preventing unauthorized access, disclosure or use of data.

Government Agencies are further subject to the requirements and restrictions contained in applicable state and federal laws protecting privacy and data security, including but not limited to the Massachusetts Fair Information Practices Act, M.G.L. c. 66A; M.G.L. c. 93H (data breaches); and M.G.L. c. 93I (data destruction).

Government Agencies requesting and receiving data from CHIA must notify CHIA of any unauthorized use or disclosure of CHIA data.

Signature:	
Printed Name:	
Title:	
Agency:	
Date:	